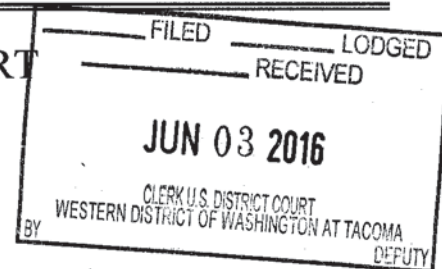


## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

See Attachment A for Premises and Vehicles to be  
Searched

Case No.

MJ16-5096

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A for Premises and Vehicles to be Searched

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B for a List of Items to be Seized.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

See Attachment C for List of  
Violations

The application is based on these facts:

See Attached Affidavit of Special Agent Joseph C. Lopez

- ☐ Continued on the attached sheet.  
☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Joseph C. Lopez, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/3/2016 908am

Judge's signature

City and state: Tacoma, Washington

David W. Christel United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

- (1) The offices of Eagle Mountain Products, Inc. including any outbuildings, located at or near 213 W. Wallace Kneeland Blvd. Shelton, WA 98584, a sole structure located immediately to the Southwest of the intersection of Highway 101 South and Wallace Kneeland Blvd. Eagle Mountain Products, Inc. is a large, metal shed that is approximately 50x100 feet and located at the Southern end of a gated large dirt lot as shown below. At the front entrance there is a sign that reads "Eagle Mountain Floral Greens Salal Beargras"



- (2) Leonar Salazar's Residence including the garage and any outbuildings, located at 3012 93<sup>rd</sup> Avenue SW, Olympia Washington 98512. The home is a single level residence with a two car garage attached as shown below. On the mailbox in front of the house reads the numbers 3012. The main entrance to the residence is through the front door;



According to Thurston County Assessor's Office Records, the property is a 3.4 acre parcel, and photos and maps show a total of five outbuildings. And any digital devices found therein.



- (3) Eulalia Salazar's Residence including the garage and any outbuildings, located at 150 S. Elderberry Ave. Forks, WA 98331. The home is a single level mobile residence, with maroon trim as shown below. The apparent entrance to the structure faces east towards the street off of a pop-out on the Southern side of the mobile home. The number 150 is displayed on a post in front of the mobile home.



- (4) 2010 Acura MDX with Washington license plate number AXY4781 and Vehicle Identification Number 2HNYD2H26AH528903;
- (5) 2005 Nissan Titan Pickup with Washington license plate number B37590T and Vehicle Identification Number 1N6AA07BX5N554954;

And any digital devices found therein.



**ATTACHMENT B**  
**EVIDENCE TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed documents); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, zip cartridges, printer buffers, smart cards, electronic notebooks, cell phones or any other storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 371 (Conspiracy to Commit Tax Evasion and to defraud the United States); 26 U.S.C. § 7201 (Tax Evasion); 26 U.S.C. § 7206(1) (Making or Subscribing False Income Tax Returns) for the time period January 2011 to the present.

- (1) All records, including but not limited to communications to or from potential purchasers or sellers, relating to any Salal, greenery, or floral distribution for the following companies:
  - Eagle Mountain Products, Inc.
- (2) All records relating to any payments or distributions to any purchasers or sellers of Salal, greenery, or floral products from or to Eagle Mountain Products, Inc., Leonar Salazar or Eulalia Salazar including but not limited to communications to purchasers, sellers and records of payments to buyers and sellers.
- (3) All corporate minute books, partnership minute books, stock registers or other records reflecting ownership of Eagle Mountain Products, Inc.
- (4) All financial statements, income tax returns, balance sheets, retained earnings, cash flow, shareholder's basis, partner's basis, payroll tax returns, excise tax returns and bookkeeper's and/or accountant's work papers used in the preparation of any such financial statements or tax returns for any of Eagle Mountain Products, Inc., Leonar Salazar, and Eulalia Salazar.
- (5) All bookkeeping and accounting records, including spreadsheets, sales journals, general ledgers, general journals, purchase journals, summaries, reconciliations, work papers relating to cash, expenditures, assets, liabilities, owner's equity, purchase of goods for resale for any of Eagle Mountain Products, Inc. or Leonar Salazar and Eulalia Salazar.
- (6) All records for any checking account, savings account, brokerage account, or credit card account for any of Eagle Mountain Products, Inc., or Leonar Salazar, and Eulalia Salazar including but not limited to all statements, deposit slips, checks deposited, checks written, wire transfers, debit and credit memos, and Forms 1099 issued.
- (7) All documents relating to the purchase, sell, rental, lease or the receipt of revenue from wholesale salal sales or from any other source, by any of Eagle Mountain Products, Inc. or Leonar Salazar, and Eulalia Salazar.

- (8) All loan records for any of Eagle Mountain Products, Inc. or Leonar Salazar, and Eulalia Salazar, including all loan applications, financial statements, credit and background investigations, loan agreements, notes or mortgages, settlement sheets, contracts, retained copies of checks issued for loans, repayment records correspondence files and internal memoranda relative to these loans.
- (9) All address books, calendars, appointment books, diaries, journals, organizers, Personal Digital Assistant "Palm Pilots" or other electronic organizers, revealing business meetings conducted by any employee of Eagle Mountain Products, Inc. or Leonar Salazar, and Eulalia Salazar.
- (10) All telephone records, including bills and toll records, for Eagle Mountain Products, Inc. or Leonar Salazar and Eulalia Salazar.
- (11) All records relating to travel outside the U.S. and the delivery of documents and other materials through the U.S. Postal Service or any common carrier, such as Federal Express, in connection with any of Eagle Mountain Products, Inc. or Leonar Salazar and Eulalia Salazar. All passports for Leonar Salazar and Eulalia Salazar.
- (12) All records, documents, keys, maps, agreements, or other items associated with any storage facilities, safety deposit boxes, mailboxes, and/or other locations where any of the foregoing evidence may be located.
- (13) All documents relating to any payments made to or money received from domestic or international sources by Leonar Salazar and Eulalia Salazar, and all documents relating to any expenditures made by Leonar Salazar and Eulalia Salazar, including all receipts for any such expenditures.
- (14) All items reflecting the income domestic and international, proceeds, expenditures or assets of Leonar Salazar and Eulalia Salazar.
- (15) Any cash located in the premises or on the persons of Leonar Salazar and Eulalia Salazar.
- (16) Digital devices and /or their components, which include, but are not limited to:
  - (a) Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;
  - (b) Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including cell phones, word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;
  - (c) Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs,

optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

(d) Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

(e) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

(f) Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

(g) Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

(17) From within the electronically stored evidence stored on or in any digital device seized pursuant to this warrant:

(a) Evidence of who used, owned or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

(b) Evidence of software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

(c) Evidence of the lack of such malicious software;

(d) Evidence of the attachment of the digital device to other storage devices or similar containers for electronic evidence;

(e) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

(f) Evidence of times the digital device was used;

(g) Passwords, encryption keys, and other access devices that may be necessary to access the digital device;



- (h) Documentation and manuals that may be necessary to access the digital device or to conduct a forensic examination of the digital device;
- (i) Any other ESI from the digital device necessary to understand how the digital device was used, the purpose of its use, who used it, and when, but limited to the individuals identified in the affidavit in support of the warrant.

THE SEIZURE OF COMPUTER SYSTEMS AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

**ATTACHMENT C**  
**List of Violations**

The search is related to violations of:

- Title 18 U.S.C. Section 371 - Conspiracy to Commit Tax Evasion and to defraud the United States
- Title 26 U.S.C. Section 7201 - Tax Evasion
- Title 26 U.S.C. Section 7206(1) - Making or Subscribing False Income Tax Returns

STATE OF WASHINGTON )  
 )  
 ) SS  
COUNTY OF PIERCE )

## I. INTRODUCTION AND AFFIANT BACKGROUND

2. I earned a Bachelor of Arts degree in accounting from a Montana State University. I attended the Criminal Investigator Training Program and the Internal Revenue Service ("IRS") Special Agent Basic Training at the Federal Law Enforcement Training Center where I received detailed training in conducting financial investigations. The training included search and seizure, violations of the Internal Revenue laws, and IRS procedures and policies in criminal investigations. Before being hired by IRS-CI, I was employed as a Revenue Agent for the IRS for approximately three years performing civil examinations of small businesses and self-employed individuals. As a Revenue Agent I received sixteen weeks of specialized training in personal, partnership, and corporate income tax, as specified in the Internal Revenue Code.

AFFIDAVIT OF JOE LOPEZ/ - 1  
USAO # 2013R00751

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE 5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970



1 alleged criminal violations, which have included: tax evasion (26 U.S.C. § 7201); filing a false  
 2 return (26 U.S.C. § 7206(1)); aiding or assisting in the preparation of false tax returns (26  
 3 U.S.C. § 7206(2)); conspiring to defraud the United States with respect to claims (18 U.S.C. §  
 4 286); false or fraudulent claims (18 U.S.C. § 287); and money laundering (18 U.S.C. §§ 1956,  
 5 1957).

6 4. I have participated in the execution of federal search warrants involving the  
 7 seizure of contraband and records relating to the concealment of assets and proceeds from  
 8 fraud, and consensual searches of records. These records included, but were not limited to,  
 9 telephone bills, personal telephone books, e-mails, photographs and letters that have identified  
 10 co-conspirators and others involved in the fraud, records pertaining to the purchase of real and  
 11 personal property, bank records, escrow records, credit card records, tax returns, business  
 12 books and records, and computer hardware and software.

13 5. I am currently conducting an investigation relating to Eagle Mountain Products,  
 14 Inc. ("EMP"), its owner Leonar Salazar ("Salazar") and his sister Eulalia Salazar ("Eulalia").  
 15 I make this Affidavit in support of an application under Rule 41 of the Federal Rules of  
 16 Criminal Procedure for a warrant to search three premises and two vehicles (collectively  
 17 "Search Locations") described below. As set forth in this Affidavit, there is probable cause to  
 18 believe that evidence, fruits, and/or instrumentalities of the following criminal violations exists  
 19 at the Search Locations: 18 U.S.C. § 371 (conspiracy to commit tax evasion and to defraud the  
 20 United States); 26 U.S.C. § 7201 (tax evasion); and 26 U.S.C. § 7206(1) (making or  
 21 subscribing false income tax returns). The items to be searched for and seized are set forth in  
 22 greater particularity in Attachment B hereto.

## 23 II. LOCATIONS TO BE SEARCHED

24 6. This Affidavit seeks authorization to search three premises ("Subject Premises")  
 25 and two vehicles ("Subject Vehicles"), and any digital devices found therein.

26 The Subject Premises are:  
 27  
 28

1 a. The offices of Eagle Mountain Products, Inc., located at or near <sup>1</sup>213 W.  
2 Wallace Kneeland Blvd. Shelton, WA 98584; and

3 b. Leonar Salazar's residence, located at 3012 93<sup>rd</sup> Ave. SW Olympia, WA  
4 98512; and

5 c. Eulalia Salazar's residence, located at 150 S. Elderberry Ave. Forks, WA  
6 98331

7 The Subject Vehicles are:

8 a. Acura MDX with Washington license plate number AXY4781 and  
9 Vehicle Identification Number 2HNYD2H26AH528903 ("Subject Vehicle 1"); and

10 b. Nissan Titan Pickup with Washington license plate number B37590T and  
11 Vehicle Identification Number 1N6AA07BX5N554954 ("Subject Vehicle 2")

12 7. The Subject Premises and Subject Vehicles are more particularly described in  
13 Attachment A to this Affidavit, which is incorporated in full by reference.

14 8. The facts in this Affidavit come from my personal observations, my training and  
15 experience, and information obtained from other agents and witnesses. Furthermore, the facts  
16 are based on my review of Federal Income Tax Returns (and related documents) filed with the  
17 IRS, records obtained from IRS computer databases, bank documents, financial records, public  
18 records, surveillance observations, and information obtained through other sources.

19 9. This affidavit is intended to establish that there is sufficient probable cause for  
20 the requested warrant and does not set forth all of my knowledge about this matter.  
21  
22  
23  
24  
25

26 \_\_\_\_\_  
27 <sup>1</sup> The address 213 W. Wallace Kneeland Blvd. Shelton, WA 98584 is the closest address to the building and property  
28 which Eagle Mountain Products, Inc. is located on. Attachment A shows a picture of the building and property that Eagle Mountain Products, Inc. is located on.

### III. SUMMARY OF INVESTIGATION

10. Since approximately February 2014, the IRS-CI of the Seattle Field Office, FBI, and other agencies have conducted an investigation of Leonar Salazar, Eagle Mountain Products, Inc. and certain individuals associated to Salazar and EMP for drug violations, money laundering, income tax evasion and filing of false tax returns. This affidavit sets forth the probable cause to support income tax and false return violations in connection with the harvest, purchase and sale of Salal<sup>2</sup>.

11. According to Washington State secretary of state records Eagle Mountain Products, Inc., a subchapter S corporation, was established in October 2005 by Leonar Salazar, Rene Salazar, and Eulalia Salazar. Tax records show Salazar is currently the 100% owner of EMP and has been since 2011. Prior to 2011, Salazar owned 70%, Rene Salazar owned 15%, and Eulalia Salazar owned 15%.

12. The investigation has established that for tax years 2013 and 2014, Eagle Mountain Products, Inc. and Leonar Salazar as 100% owner have evaded the reporting of approximately \$1.7 million in gross receipts. EMP significantly under-reported its gross receipts as well as its ordinary income on its federal tax returns. For tax years 2013 and 2014, the under-reported gross receipts should have passed-through as earnings of EMP which were not reported to the IRS as taxable income by Salazar or Eulalia. During those years Salazar and Eulalia reported limited earnings as employees of EMP. As described in this Affidavit, the analysis of the cash flow into and out of the EMP bank accounts further supports probable cause to believe the crimes cited in this Affidavit were committed.

13. The under-reporting of corporate receipts, profits and individuals' income, as well as the use of cash transactions to disguise true corporate earnings and individuals' income relates to the tax evasion and false income tax return violations, pursuant to 26 U.S.C.

---

<sup>2</sup> Salal is thick, tough, egg-shaped leaves which are shiny and dark green on the upper surface, and rough and lighter green on the lower. In the Pacific Northwest, the harvesting of Salal is the heart of a large industry which supplies cut evergreens worldwide for use in floral arrangements.



1 §§ 7201, 7206. Finally, because the investigation has established that multiple individuals  
2 may have agreed to commit certain of the above crimes, the conspiracy provisions are also  
3 implicated.

#### 4 IV. THE INVESTIGATION

##### 5 A. Subjects and Entities

###### 6 LEONAR DIMAS AKA: AARON SALAZAR ("SALAZAR")

7 14. Salazar was born in Mexico in or around 1964. Salazar is not a U.S. Citizen.  
8 Salazar is single and is known to have at least one child. Salazar is the 100% owner of Eagle  
9 Mountain Products, Inc.

###### 10 EULALIA SALAZAR ("EULALIA")

11 15. Eulalia was born in Mexico in or around 1973. Eulalia is not a U.S. Citizen.  
12 Eulalia is the sister to Leonar Salazar. Eulalia is married and known to have at least three  
13 children. Eulalia is working with Salazar and actively shares control of the EMP bank  
14 accounts.

###### 15 EAGLE MOUNTAIN PRODUCTS, INC. ("EMP")

16 16. Eagle Mountain Products was established in October 2005 by Salazar, and the  
17 company is still currently active. Salazar is listed on Washington State Secretary of State  
18 records as the governing person holding all offices of the corporation. The EMP Company's  
19 federal tax returns identify the business activity as Farmer and the product of service is Bush  
20 or better known as Salal. According to federal tax records, Salazar is the sole shareholder of  
21 EMP.

##### 22 B. Salal Industry

23 17. Over the course of the investigation I have learned about the Salal industry  
24 through research online and an interview with a local major floral company. Salal is a plant  
25 with thick, tough, egg-shaped leaves which are shiny and dark green on the upper surface, and  
26 rough and lighter green on the lower and come in different lengths; Tips, Long, and Short.  
27 Salal only grows in the Northwest between British Columbia and the Northern Tip of  
28

1 California. In the Pacific Northwest, the harvesting of Salal is the heart of a large industry  
2 which supplies cut evergreens worldwide for use in floral arrangements.

3 18. A permit is needed to pick Salal whether harvested from private or federal land.  
4 Any picker can obtain a permit from the local assessor's office to pick on federal land or once  
5 they have approval from the property owner where they plan on picking the Salal. Some large  
6 Salal companies will lease hundreds of acres of land which gives them the only right to pick  
7 on that land. Pickers will take rubber bands and ropes with them when they go pick the Salal.  
8 The rubber bands are used to secure a handful of Salal and the rope is used to tie up bundles of  
9 handfuls. Pickers are paid by the handful of Salal, which can vary in price from \$.45 to \$1.00,  
10 depending on demand and type. Salal pickers could be independents, contractors, or  
11 employees of Salal companies. Most pickers are contractors which are hauled around from  
12 area to area in a twelve-passenger van. The Salal bundles they pick are tagged with their name  
13 and thrown in the back of a truck. Pickers are paid daily or weekly, with most small  
14 companies paying cash and the large floral companies paying by check so they have a record  
15 of payment.

16 19. Once the Salal is brought back to the Salal shed it is boxed up and usually sent  
17 overseas to Europe. Approximately 80% of all Salal harvested is exported to European  
18 countries. Cases of Salal are usually comprised of 25 handfuls. A case of Salal depending on  
19 quality, age, and the market, could sell for \$16 to \$36 per case, indicating an average gross  
20 margin of 43%. Salal that is sold to European Vendors is either shipped out of the Port of  
21 Tacoma, trucked to Vancouver, BC to be placed on rail to the East Coast for shipping, or air  
22 freighted out of SeaTac airport, all depending on time of season. Containers that are shipped  
23 overseas could contain up to a 1,000 cases of Salal. The containers are hand packed to allow  
24 more room for the Salal and save on weight. A shrink-wrapped pallet air freighted to Europe  
25 would contain 32 to 40 cases. Freight costs whether by sea or air are usually paid by the  
26 purchaser.

**C. Eagle Mountain Products Company's Federal Tax Returns**

20. Eagle Mountain Products, Inc. filed S corporation federal tax returns (Form 1120S) for the years 2011 through 2015. An S corporation is one that elects to pass corporate income, losses, deductions and credits through to its shareholders for federal tax purposes. Shareholders of S corporations report the flow-through of income and losses on their personal tax returns and are assessed tax at their individual income tax rates. According to IRS records, Carlota Herrera at KL Computax Inc. has prepared the EMP Company Form 1120S tax return since at least 2011. A review of IRS records shows Carlota Herrera also prepared 2012-2015 personal federal tax returns for Salazar and 2011 for Eulalia<sup>3</sup>. Salazar electronically signed each of the EMP Company's S Corporation tax returns for tax years 2011 through 2015 as president of the company. The returns are filed with the IRS electronically by Carlota Herrera.

21. A summary of EMP Company's S Corporation tax returns for the years 2011 through 2015 are shown below:

*Fig. 1*

Tax Year	Gross Receipts	Cost of Goods Sold ("COGS")	Gross Margin Percentage ("Markup")	Total Income	Total Deductions	Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar)
2011	\$ 1,854,229	\$1,542,085	20%	\$ 312,144	\$ 260,109	\$ 52,035
2012	\$ 3,538,823	\$3,152,065	12%	\$ 386,758	\$ 320,103	\$ 66,655
2013	\$ 2,790,529	\$2,294,886	22%	\$ 495,643	\$ 463,350	\$ 32,293
2014	\$ 2,818,645	\$2,434,521	16%	\$ 384,124	\$ 348,437	\$ 35,687
2015	\$ 3,818,569	\$3,275,748	17%	\$ 542,821	\$ 513,869	\$ 28,952
<b>Totals</b>	<b>\$14,820,795</b>	<b>\$12,699,305</b>	<b>17%</b>	<b>\$2,121,490</b>	<b>\$1,905,868</b>	<b>\$215,622</b>

22. The gross receipts reported on EMP Company's 2013 and 2014 federal tax returns are believed to be false based on the amounts deposited to the EMP bank accounts for

<sup>3</sup> Eulalia self-prepared her federal tax returns for tax years 2012 through 2014.



each year. The majority of deposits are checks and wires from floral companies either locally or overseas. Fig 2 below shows the difference between deposits from floral companies and gross receipts reported by EMP for 2013 and 2014.

*Fig. 2*

<b>Year</b>	<b>Gross Receipts As reported on EMP Company's Federal Tax Returns</b>	<b>Total Deposits to EMP Company's Bank Accounts for the same years (Floral company checks and wires)</b>	<b>Difference between Gross Receipts as reported on EMP Company's federal tax returns and total deposits to EMP Company's Bank Accounts for the same years</b>
2013	\$2,790,595	\$4,258,229	\$1,467,634
2014	\$2,818,645	\$3,088,359	\$ 269,714
<b>Total</b>	<b>\$5,609,240</b>	<b>\$7,346,588</b>	<b>\$1,737,348</b>

23. The Cost of Goods Sold ("COGS") reported on EMP Company's 2011 through 2015 federal tax returns are believed to be false based on EMP Company's low average gross margin along with the total amount of cash withdrawals from the EMP bank accounts for each year. Based on the cost of goods sold and the gross receipts reported on EMP Company's federal tax returns 2011-2015, the company charged an average mark-up of 17% (Gross Revenues/COGS). As discussed in paragraph 19, the average mark-up on Salal is around 43%. Figure 3 below shows the difference between the gross margins (markups) on EMP Company's federal tax returns and the average 43% mark-up for the Salal industry.

Fig. 3

Year	Cost of Goods Sold ("COGS") As reported on EMP Company's federal tax returns	Estimated Cost of Goods Sold using Salal industry average markup of 43% (Gross Receipts from Fig. 1/1.43%)	Difference between COGS as reported on EMP Company's federal tax returns and the Salal industry average markup
2011	\$ 1,542,085	\$ 1,296,664	\$ 245,421
2012	\$ 3,152,065	\$ 2,474,701	\$ 677,364
2013	\$ 2,294,886	\$ 1,951,419	\$ 343,467
2014	\$ 2,434,521	\$ 1,971,080	\$ 463,441
2015	\$ 3,275,748	\$ 2,670,328	\$ 605,420
<b>Total</b>	<b>\$12,699,305</b>	<b>\$10,364,192</b>	<b>\$2,335,113</b>

24. Applying the "Approximate Cost of Goods Sold using Salal industry average markup of 43%" as shown in fig. 3 as actual COGS for EMP Company's tax returns for 2011 through 2015 would equate to the following approximate gross receipts as shown in fig. 4.

Fig. 4

Year	Gross Receipts As reported on EMP Company's Federal Tax Returns	Estimated Cost of Goods Sold using Salal industry average markup of 43% (Gross Receipts from Fig. 1/1.43%)	Estimated Total Income if using Salal industry average markup of 43%
2011	\$ 1,854,229	\$1,296,664	\$ 557,565
2012	\$ 3,538,823	\$2,474,701	\$1,064,122
2013	\$ 2,790,529	\$1,951,419	\$ 839,110

2014	\$ 2,818,645	\$1,971,080	\$ 847,565
2015	\$ 3,818,569	\$ 2,670,328	\$1,148,241
<b>Total</b>	<b>\$14,820,795</b>	<b>\$10,364,192</b>	<b>\$4,456,603</b>

25. Applying the "Estimated Total Income if using Salal industry average markup" as shown in fig. 4 less total deductions as shown on EMP Company's tax returns for 2011 through 2015 would equate to the following approximate Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar) shown in fig. 5.

Fig. 5

Tax Year	Gross Receipts as shown on EMP tax returns	Estimated COGS as shown in fig. 4	Estimated Gross Margin Percentage ("Markup")	Estimated Total Income as shown in fig. 4	Total Deductions as shown on EMP tax returns	Estimated Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar)
2011	\$ 1,854,229	\$1,296,664	43%	\$ 557,565	\$ 260,109	\$ 297,456
2012	\$ 3,538,823	\$2,474,701	43%	\$1,064,122	\$ 320,103	\$ 744,019
2013	\$ 2,790,529	\$1,951,419	43%	\$ 839,110	\$ 463,350	\$ 375,760
2014	\$ 2,818,645	\$1,971,080	43%	\$ 847,565	\$ 348,437	\$ 499,128
2015	\$ 3,818,569	\$2,670,328	43%	\$1,148,241	\$ 513,869	\$ 634,372
<b>Totals</b>	<b>\$11,002,226</b>	<b>\$7,693,864</b>	<b>43%</b>	<b>\$4,456,603</b>	<b>\$1,905,868</b>	<b>\$2,550,735</b>

26. The difference between "Estimated Ordinary Income Gain/Loss to Flow-Through to Shareholders" as shown in fig. 5 and actual "Ordinary Income Gain/loss to Flow-Through Shareholders" as shown in fig. 1 would be unreported ordinary income as shown in fig. 6.

Fig. 6

Year	Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar) fig. 1	Estimated Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar) fig. 5	Estimated unreported Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar)
2011	\$ 52,035	\$ 297,456	\$245,421
2012	\$ 66,655	\$ 744,019	\$677,364
2013	\$ 32,293	\$ 375,760	\$343,467
2014	\$ 35,687	\$ 499,128	\$463,441
2015	\$ 28,952	\$ 634,372	\$605,420
<b>Total</b>	<b>\$215,622</b>	<b>\$2,550,735</b>	<b>\$2,335,113</b>

27. Based on the above analysis, approximately \$2.3 million of "Ordinary Income Gain/Loss to Flow-Through to Shareholders (Salazar)" fig. 6 has not been reported on EMP Company's 2011 through 2015 federal tax returns.

#### **D. Leonar Salazar Personal Tax Returns**

28. In addition to the analysis of EMP Company's federal tax returns and the estimated ordinary income not reported for 2011 through 2015, I believe probable cause of the enumerated crimes exists based on an analysis of the personal tax returns of Leonar Salazar in conjunction with the flow of cash out of EMP bank accounts controlled by Salazar and Eulalia. As described in more detail below, approximately \$6.8 million in cash was withdrawn from EMP accounts between January 1, 2011 and November 2015.

29. A summary of the Leonar Salazar's Head of Household Form 1040 personal tax return information for the years 2011 through 2015 is shown below:



Fig. 7

Tax Year	Wages	Other Income	Adjusted Gross Income	Taxable Income	Earned Income Credit <sup>4</sup>	Income Tax Due/Refund
2011	\$20,700	\$0.00	<b>\$20,700</b>	\$1,100	\$4,262	(\$8,136)
2012	\$6,600	\$66,655	<b>\$73,255</b>	\$59,955	\$0.00	\$7,345
2013	\$19,800	\$32,143	<b>\$51,943</b>	\$35,193	\$0.00	\$1,240
2014	\$29,100	\$35,687	<b>\$64,787</b>	\$47,787	\$0.00	\$2,479
2015	\$40,600	\$28,952	<b>\$69,552</b>	\$53,302	\$0.00	\$1,375

30. The reported wages in 2011, 2012, 2013, 2014, and 2015 are from EMP.

31. During 2011 Salazar was the 100% shareholder of EMP which reported ordinary income of \$52,035. Salazar as 100% shareholder was supposed to report the \$52,035 as other income on his personal federal tax return which he did not.

32. The income reported on Salazar's personal tax returns appears to be false based on the analysis of financial and other records obtained.

#### **E. Eulalia Salazar Personal Tax Returns**

33. In addition to the analysis of EMP Company's federal tax returns and the estimated ordinary income not reported for 2011 through 2015, I believe probable cause of the enumerated crimes exists based on an analysis of the personal tax returns of Eulalia Salazar in conjunction with the flow of cash out of EMP bank accounts controlled by Salazar and Eulalia. As described in more detail below, approximately \$6.8 million in cash was withdrawn from EMP accounts between January 1, 2011 and November 2015.

34. A summary of the Eulalia Salazar's Married<sup>5</sup> Form 1040 personal tax return information for the years 2011 through 2015 is shown below:

<sup>4</sup> EITC, Earned Income Tax Credit, is a benefit for working people who have low to moderate income. It reduces the amount of tax owed and may also provide a refund. In Tax Year 2014, for a family with two qualifying children to obtain the Earned Income Tax Credit, Adjusted Gross Income (AGI) must be less than \$43,756 (\$49,186 married filing jointly).

<sup>5</sup> For tax years 2011 and 2012, Eulalia lists her spouse as J Ensastegui-Ferreya. For tax years 2013 and 2015 Eulalia is listed as a spouse to O Ensastegui-Ferreya as primary on his federal tax return. For tax year 2014 Eulalia files a married federal tax return and lists O Ensastegui-Ferreya as her spouse. Per IRS records, J Ensastegui-Ferreya and O Ensastegui-Ferreya are believed to be brothers and whether or not Eulalia is or was married to both brothers is unknown.

Fig. 7

Tax Year	Wages	Other Income	Adjusted Gross Income	Taxable Income	Earned Income Credit	Income Tax Due/Refund
2011	\$26,240	\$3,600 <sup>6</sup>	\$29,840	\$0.00	\$0.00	(\$3,074)
2012	\$28,189	\$0.00	\$28,189	\$0.00	\$0.00	(\$6,346)
2013	\$17,030	\$0.00	\$17,030	\$0.00	\$0.00	(\$2,156)
2014	\$10,500	\$0.00	\$10,500	\$0.00	\$0.00	(\$1,155)
2015	\$15,359	\$0.00	\$15,359	\$0.00	\$0.00	(\$1,883)

35. The Form W-2's attached to Eulalia's married filing joint tax returns reported wages in 2011, 2012 and 2015 for Eulalia, J Ensastegui-Ferreya, and O Ensastegui-Ferreya from multiple employers including EMP. The reported wages in 2013 and 2014 for Eulalia and O Ensastegui-Ferreya are from EMP.

36. The income reported on Eulalia's married filing joint federal personal tax returns appears to be false based on the analysis of financial and other records obtained.

#### F. Bank Account Analysis

##### 1. Eagle Mountain Products, Inc. Company Bank Accounts

37. Bank of America records show Leonar Salazar opened account no. xxxx-8315 in the name of Eagle Mountain Products, Inc. on October 11, 2005. Eulalia is shown as the only additional authorized signor on the account. In account opening paperwork Salazar lists his business as Salal.

38. Records for Bank of America account no. xxxx-8315 between January 2011 and July 2015<sup>7</sup> show that the majority of deposits are checks and wires from floral companies either locally or overseas. The majority of withdrawals are cash, payments to third party individuals (by check), gas, office rent, accounting, department stores, and restaurants. The

<sup>6</sup> The other income is rent received by Eulalia from the Quileute Tribal Council.

<sup>7</sup> Salazar closed Bank of America account no. xxxx-8315 in July 2015.

1 checks written to third parties are believed to be for the purchase of Salal and are between  
2 \$500 and \$5,000<sup>8</sup>.

3 39. Records show multiple withdrawals by Salazar and Eulalia of large amounts of  
4 cash.

5 40. Records show multiple wire transfers to another EMP bank account located at  
6 Sterling Bank.

7 41. Records show multiple online transfers to third party accounts.

8 42. Records show both Salazar and Eulalia sign the checks payable to the third  
9 parties.

10 43. Fig. 8 below summarizes the deposits and withdrawals<sup>9</sup> to account no. xxxx-  
11 8315 between 2011 and 2015.

12 *Fig. 8*

Year	Check Deposits	Wire Deposits (Overseas)	Check Withdrawals	Wire Withdrawals	Cash Withdrawals	ATM Withdrawals
2011	\$1,850,531	\$ 0.00	\$1,031,785	\$ 0.00	\$ 466,000	\$ 4,620
2012	\$1,462,270	\$ 449,888	\$ 126,533	\$ 109,000	\$1,464,950	\$ 12,682
2013	\$1,598,768	\$2,335,325	\$ 215,567	\$1,190,500	\$2,131,555	\$ 36,292
2014	\$ 746,965	\$2,341,395	\$ 239,593	\$ 924,200	\$1,166,687	\$ 48,822
2015 <sup>10</sup>	\$ 352,972	\$1,153,635	\$ 184,114	\$ 474,500	\$ 789,531	\$ 9,331
<b>Totals</b>	<b>\$6,011,506</b>	<b>\$6,280,243</b>	<b>\$1,797,592</b>	<b>\$2,698,200</b>	<b>\$6,018,723</b>	<b>\$111,747</b>

25 <sup>8</sup> The majority of these checks are cashed for cash by the third party.

26 <sup>9</sup> Additional withdrawals from account xxxx-8315 not shown in fig. 8 include debit card purchases, online transfers to 3<sup>rd</sup>  
27 party accounts, and a small amount of wires to Mexico.

28 <sup>10</sup> Bank records are a partial year as account was closed in July 2015.



1        44. Additional research of the cash withdrawals shown in fig. 8 of approximately \$6  
 2 million reveals \$1.08 million being withdrawn through 510 transactions of equal to or less than  
 3 \$5 thousand.

4        45. Sterling Bank records show Salazar opened account no. xxxx-4497 in the name  
 5 of Eagle Mountain Products, Inc. on January 26, 2012<sup>11</sup>. Eulalia is shown as the only  
 6 additional authorized signor on the account.

7        46. Records for Sterling Bank account no. xxxx-4497 between January 2012 and  
 8 November 2015<sup>12</sup> show that the majority of deposits are checks from local floral companies,  
 9 wires from overseas, wires from EMP Company's Bank of America account no. xxxx-8315 or  
 10 wires from EMP Company's Our Community Credit Union account no. xxxx-5598. The  
 11 majority of withdrawals are cash, payments to third party individuals (by check), gas, office  
 12 rent, accounting, and restaurants. The checks written to third parties are believed to be for the  
 13 purchase of Salal and are between \$500 and \$5,000.<sup>13</sup>

14        47. Records show multiple cash withdrawals by Salazar and Eulalia.

15        48. Records show both Salazar and Eulalia sign the checks payable to the third  
 16 parties.

17        49. Fig. 9 below summarizes the deposits and withdrawals<sup>14</sup> to account no. xxxx-  
 18 4497 between 2012 and 2015.

24 <sup>11</sup> Umpqua Bank absorbed Sterling Bank in 2014 with all EMP account information staying the same.

25 <sup>12</sup> Bank records for December 2015 have not been received to date.

26 <sup>13</sup> The majority of these checks are cashed for cash by the third party.

27 <sup>14</sup> Additional withdrawals from account xxxx-4497 not shown in fig. 9 include debit card purchases and, online transfers to  
 28 3<sup>rd</sup> party accounts, and a small amount of wires to Mexico.



Fig. 9

Year	Check Deposits	Wire Deposits (Overseas)	Wire Deposits (From BofA 8315 or OCCU 5598)	Check Withdrawals	Cash Withdrawals	ATM Withdrawals
2012	\$553,266	\$1,151,678	\$ 109,000	\$1,133,872	\$633,815	\$ 7,660
2013	\$394,424	\$ 39,962	\$1,190,500	\$1,539,572	\$ 87,310	\$26,170
2014	\$ 0.00	\$ 0.00	\$ 924,200	\$ 925,863	\$ 95,840	\$ 9,850
2015	\$ 0.00	\$ 0.00	\$ 474,500	\$ 665,020	\$ 39,050	\$ 6,050
<b>Totals</b>	<b>\$947,690</b>	<b>\$1,191,640</b>	<b>\$2,698,200</b>	<b>\$4,264,327</b>	<b>\$856,015</b>	<b>\$49,730</b>

50. Additional research of the cash withdrawals shown in fig. 9 of approximately \$856 thousand reveals \$295 thousand being withdrawn through 156 transactions of equal to or less than \$5 thousand.

51. Our Community Credit Union ("OCCU") records show Salazar opened account no. xxxx-5598 in the name of Eagle Mountain Products, Inc. on June 5, 2015. Salazar used his personal residence address of 3012 93<sup>rd</sup> Ave. SW Olympia, WA 98512 as the physical address for Eagle Mountain Products, Inc. Salazar is shown as the only signor on the account.

52. Records for OCCU account no. xxxx-5598 between June 2015 and December 2015 show that the majority of deposits are checks from local floral companies and wires from overseas. The majority of withdrawals are cash, payments to third party individuals (by check), gas, office rent, accounting, and restaurants. The checks written to third parties are believed to be for the purchase of Salal and are between \$500 and \$5,000.<sup>15</sup>

53. Records show multiple cash withdrawals by Salazar.

54. Records show Salazar and Eulalia both signed the checks payable to the thirds parties even though Salazar is the only authorized signor on the account.

<sup>15</sup> The majority of these checks are cashed for cash by the third party.

55. Fig. 10 below summarizes the deposits and withdrawals<sup>16</sup> to account no. xxxx-5598 between June 2015 and December 2015.

Fig. 10

Year	Check Deposits	Wire Deposits (Overseas)	Check Withdrawals	Cash Withdrawals	ATM Withdrawals
2015	\$301,734	\$1,736,443	\$1,556,878	\$202,157	\$9,815

56. Additional research of the cash withdrawals shown in fig. 9 of approximately \$202 thousand reveals \$63 thousand being withdrawn through 29 transactions of equal to or less than \$5 thousand.

57. EMP has two additional checking and two savings accounts, Peninsula Credit Union account no. xxxx-9277 and account no. xxxx-0238, Bank of America account no. xxxx-0509 and Sterling Bank no. xxxx-1424, respectively. All four accounts have minimal activity in comparison to the main EMP business accounts described above.

## 2. Leonar Salazar Bank Accounts

58. In review of bank records, we located no less than ten checking and savings accounts owned by Salazar between 2011 and 2015. Eight of the ten accounts were closed by Salazar prior to or during 2013. One of the two remaining accounts was Wells Fargo checking account no. xxxx-8407 which was closed in February 2015. The only remaining account open is at Peninsula Credit Union savings account no. xxxx-5826. All ten checking and savings accounts have been reviewed with minimal activity revealed in the accounts. Between 2011 and 2014, Salazar made the most deposits and withdrawals from his Wells Fargo account no. xxxx-8407. In review of Wells Fargo account no. xxxx-8407 Salazar would deposit on average \$20 thousand a year through cash, EMP payroll checks, or third party checks.

<sup>16</sup> Additional withdrawals from account xxxx-5598 not shown in fig. 10 include debit card purchases and online transfers to 3<sup>rd</sup> party accounts.

Withdrawals from the account included; hotels, department stores, vehicle rentals, gas, restaurants, liquor, utilities, parking, and ATM withdrawals.

### 3. Eulalia Salazar Bank Accounts

59. In review of bank records, we located seven accounts at First Federal all open during or after June 2011. All seven accounts have been reviewed with minimal activity revealed in five of the accounts. The two accounts with the most activity, no. xxx-0878 and no. xxx-5410 have been analyzed for tax years 2014 and 2015 as shown in fig. 11 and fig. 12.

*Fig. 11*

Account no. xxxx-0878<sup>17</sup>

Year	Cash/Check Deposits	Online Transfer Deposits	Wire Deposits	Cash Withdrawals	Cashier's Check Withdrawal	Online Transfer Withdrawals
2014	\$37,641	\$23,400	\$78,100	\$ 93,120	\$67,000	\$33,180
2015	\$37,624	\$18,400	\$ 0.00	\$ 26,305	\$ 0.00	\$17,258
<b>Totals</b>	<b>\$75,265</b>	<b>\$41,800</b>	<b>\$78,100</b>	<b>\$119,425</b>	<b>\$67,000</b>	<b>\$50,438</b>

*Fig. 12*

Account no. xxxx-5410<sup>18</sup>

Year	Cash/Check Deposits	Online Transfer Deposits	Cash Withdrawals	Online Transfer Withdrawals	Debit Card Withdrawals
2014	\$28,310	\$33,708	\$0.00	\$20,149	\$12,049
2015	\$25,287	\$17,902	\$200	\$17,350	\$14,804
<b>Totals</b>	<b>\$53,597</b>	<b>\$51,610</b>	<b>\$200</b>	<b>\$37,499</b>	<b>\$26,853</b>

<sup>17</sup> Account beginning balance on 1/1/2014 was \$59,558.06.

<sup>18</sup> Account beginning balance on 1/1/2014 was \$1,272.59.



1        60. As shown in fig. 7, Eulalia and her spouse reported total income in 2014 of  
2 \$10,500 and 2015 of \$15,359. As shown in fig. 11 and 12, Eulalia and her spouse's banking  
3 activity does not match what their federal tax returns are showing.

4        **G. Additional Information Regarding Subject Premises and Vehicles**

5                *Subject Premises*

6                *Eagle Mountain Products, Inc.*

7        61. Based on physical surveillance, investigators have established that at or near 213  
8 W. Wallace Kneeland Blvd. Shelton, WA 98584 is the business of Eagle Mountain Products,  
9 Inc. FBI agents and I along with others have gone to the business address and independently  
10 confirmed that the office of Eagle Mountain Products, Inc. is located at or near 213 W.  
11 Wallace Kneeland Blvd. Shelton, WA 98584. FBI agents and I along with others have  
12 observed Salazar driving to and from Eagle Mountain Products, Inc. located at or near 213 W.  
13 Wallace Kneeland Blvd. Shelton, WA 98584 on several surveillance operations.

14                *Leonar Salazar Personal Residence*

15        62. Based on documentary evidence and physical surveillance, investigators have  
16 established that 3012 93rd Avenue SW Olympia, WA 98512 is Salazar's personal residence.  
17 Washington State Department of Licensing has a Vehicle Certificate of Ownership (Title)  
18 Application on file from January 6, 2016 listing 3012 93<sup>rd</sup> Avenue SW Olympia, WA 98512 as  
19 Salazar's primary residence. FBI agents and I along with others have gone to this address and  
20 independently confirmed that Salazar's personal residence is located at 3012 93rd Ave. SW  
21 Olympia, WA 98512. FBI agents and others have personally seen Salazar depart from the  
22 residence at 3012 93<sup>rd</sup> Ave. SW Olympia, WA 98512.

23                *Eulalia Salazar Personal Residence*

24        63. FBI agents and I have driven to Forks and independently confirmed that  
25 Eulalia's personal residence is located at 150 S. Elderberry Ave. Forks, WA 98331. Eulalia's  
26 husband Osvaldo Ensastegui Ferreyra has his Washington driver's license and two vehicles  
27 registered to the 150 S. Elderberry Ave. Forks, WA address. FBI agents and I have seen both  
28

1 of Eulalia's husband's vehicles parked in the driveway at 150 S. Elderberry Ave. Forks, WA  
2 98331.

3 ***Subject Vehicle 1***

4 64. A Washington DOL Vehicle Title Application/Registration Certificate dated  
5 January 25, 2016 lists Salazar as the registered owner of an Acura MDX, which was assigned  
6 Washington license plate number AXY4781 with Vehicle Identification Number  
7 2HNYD2H26AH528903 as that on Salazar's application with an address of 3012 93<sup>rd</sup> Ave.  
8 SW Olympia, WA 98512. On May 18, 2016, agents observed Salazar depart from his  
9 residence at 3012 93<sup>rd</sup> Ave. SW Olympia, WA 98512 in a white Acura MDX, WA plate  
10 AXY4781. Agents followed Salazar to a business located at the end of Wallace Blvd. just  
11 west of Hwy 101 in Shelton, WA, known to be Eagle Mountain Products, Inc. Agents  
12 observed Salazar open the front gate then drive to the building where he exited his vehicle and  
13 entered the business. Approximately 15 minutes later, agents observed Salazar exit the  
14 business, get back in the Acura MDX which he proceeded to drive to Heritage Bank located at  
15 301 E. Wallace Kneeland Blvd. Agents observed Salazar exit the vehicle carrying unidentified  
16 paperwork and walked into Heritage Bank. Approximately 15 minutes later Salazar exits  
17 Heritage Bank, gets back in the Acura MDX where he proceeds to drive to Wells Fargo Bank  
18 located at 1010 Sleater Kinney Rd in Lacy, WA, where Salazar parked and entered the bank.  
19 Approximately 7 minutes later Salazar exited Wells Fargo Bank, gets back in the Acura MDX  
20 where he proceeds to drive to Mortgage One Northwest located at 8120 Freedom Ln NE in  
21 Lacy, WA, where Salazar parked and entered the building. Approximately 45 minutes later  
22 Salazar exited the building, gets back in the Acura MDX where he proceeds to drive to Wells  
23 Fargo Bank located at 1419 Marvin Rd in Lacy, WA, where he parked and entered the bank.

24 ***Subject Vehicle 2***

25 65. On September 14, 2014, agents observed Salazar in a white Nissan Titan pickup  
26 truck, bearing Washington plate B37590T arriving at the EMP business located at 213 W.  
27 Wallace Kneeland Blvd. Shelton, WA 98584. The Nissan Titan has a Vehicle Identification  
28 Number of 1N6AA07BX5N554954 and is registered to Salazar with an address of 3012 93<sup>rd</sup>

1 Ave. SW Olympia, WA 98512. During several hours of surveillance, the agents observed  
2 Salazar driving the Nissan Titan from EMP to a nearby Bank of America branch, which he  
3 entered and remained within for approximately 42 minutes, before returning to EMP. Later,  
4 Salazar again departed EMP in the Nissan Titan and drove to a nearby Heritage Bank, which  
5 he entered and remained in for approximately six minutes, before returning to EMP. Salazar  
6 later departed EMP and returned to his residence at 3012 93<sup>rd</sup> Ave. SW Olympia, WA 98512.  
7 More recently, on February 4, 2016, a Detective from Mason County Sheriff's Office  
8 conducted surveillance of the Salazar's residence located at 3012 93<sup>rd</sup> Ave. SW Olympia, WA  
9 98512. The detective observed the Nissan Titan depart the residence, which the detective  
10 followed until it arrived at EMP.

11 **H. Observations about Items Likely to be found at Search Locations**

12 66. I believe that there will be evidence of the above-described crimes at the  
13 business and residence locations, and in Subject Vehicle 1 and 2 because individuals who  
14 attempt to conceal their true income, the true income of companies they control and the true  
15 ownership of their assets will keep notes and correspondence and will maintain books and  
16 records of their financial activity, such as receipts for expenditures by cash and check, money  
17 orders and cashier's checks, bank records, loan documents evidencing the obtaining, secreting,  
18 transfer, or concealment of assets and the obtaining, secreting, transfer, concealment and  
19 expenditure of money, personal tax returns with supporting documentation, and other financial  
20 documents at their place of residence or vehicles, where the individual has ready access to  
21 these documents. Specifically, the office of Eagle Mountain Products is the location used in  
22 all communications with state, federal taxation and licensing authorities and where I and  
23 others have observed the sorting and storage of Salal. The Salazar residence is the location  
24 where FBI agents and others have regularly observed Salazar enter and leave. Salazar has  
25 been observed by FBI agents and others driving vehicles 1 and 2 from his residence to the  
26 offices of Eagle Mountain Products.



1       67. Based upon my training, experience and participation in this and other financial  
2 investigations involving criminal tax violations and conspiracy to defraud the government, and  
3 based upon my conversations with other experienced special agents who have participated in  
4 similar investigations, I know:

5           a. that businesses typically retain accounting books and records at their  
6 business location;

7           b. that such books and records are made in an attempt to trace or track the  
8 flow of funds into and out of the business, to and from owners, investors, lenders, suppliers,  
9 customers and others;

10          c. that such books and records are used as the basis for the preparation of  
11 financial statements and also for the preparation of tax returns due to federal, state, and local  
12 taxing authorities;

13          d. that such books and records are ordinarily kept and retained at the place  
14 of business for extended periods of time, often several years, for a number of reasons, one of  
15 which is to provide documentation and evidence in support of shareholder and partner basis or  
16 investment, asset liability, revenue and expense transactions if questioned by IRS auditors, or  
17 other taxing authorities;

18          e. that individuals who attempt to conceal their true income, the true income  
19 of companies they control and the true ownership of assets often retain at their business  
20 location, and at their personal residence, records with false entries, such as nominee names,  
21 altered dates, altered amounts, altered classifications and altered descriptions of business  
22 transactions;

23          f. that individuals who attempt to conceal their true income, the true income  
24 of the companies they control and true ownership of assets retain at their business location,  
25 and at their personal residence, secret bank, brokerage, and other financial institution account  
26 records, in some cases both foreign and domestic, that document the flow of funds into and out  
27 of the business;

28          g. that individuals who attempt to conceal their true income, the true income  
of companies they control and the true ownership of assets often retain at their business  
location, and at their personal residence, a separate set of accounting records that document  
sources of income not reported to taxing authorities;

h. that individuals who attempt to conceal their true income, the true income  
of companies they control and the true ownership of assets often retain at their business

1 location, and at their personal residence, records relating to the identity of undisclosed  
2 principals and related party transactions;

3 i. that individuals who attempt to conceal their true income, the true income  
4 of companies they control and the true ownership of assets often retain at their business  
5 location, and at their personal residence, books and records evidencing the obtaining,  
6 secreting, transfer or concealment of assets and the obtaining, secreting, transfer, concealment  
and expenditure of money, where that individual has ready access to these documents; and

7 j. that individuals who file personal income tax returns will often maintain  
8 copies of those returns, along with supporting work papers and other documentation relating to  
those returns.

9 k. that individuals who own or benefit from cash intensive businesses that  
10 commit tax evasion often hide cash from the government by not depositing it in the bank  
11 and/or by structuring the deposits and withdrawals (depositing cash in amounts less than  
12 \$10,000). They often keep cash hoards in safes or at other locations at home or business.  
13 They often make business and personal purchases with cash (rather than credit cards or  
14 checks) as the cash has not been deposited in the bank and therefore is not recorded by a third-  
party record.

## 15 V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

16 68. Records of the type described in the preceding paragraph are also often stored on  
17 digital devices. Persons engaged in fraudulent tax schemes often maintain such records for  
18 long periods of time, particularly when they are involved in ongoing criminal conduct. There  
19 are many reasons why criminal offenders maintain evidence for lengthy periods of time. The  
20 evidence may appear innocuous at first glance (e.g. financial, credit card and banking  
21 documents, travel documents, receipts, documents reflecting purchases of assets, personal  
22 calendars, telephone and address directories, check books, videotapes and photographs, utility  
23 records, ownership records, letters and note, tax returns and financial records, escrow files,  
24 telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and  
25 software), but have significance and relevance when considered together and in light of other  
26 evidence. The criminal offender may no longer realize he or she still possesses the evidence,  
27 or may believe that law enforcement would not be able to obtain a warrant to seize the  
28 evidence. The criminal offender may also be under the mistaken belief that he or she has



1 deleted, hidden, or otherwise destroyed computer-related evidence, but which evidence may  
2 yet be retrievable by a trained forensic computer expert.

3 69. As described above and in Attachment B, this application seeks permission to  
4 search for evidence, fruits and/or instrumentalities that might be found at the search locations  
5 described in attachment A, in whatever form they are found. One form in which the evidence,  
6 fruits, and/or instrumentalities might be found is data stored on digital devices<sup>19</sup> such as  
7 computer hard drives or other electronic storage media.<sup>20</sup> Thus, the warrant applied for would  
8 authorize the seizure of digital devices or other electronic storage media or, potentially, the  
9 copying of electronically stored information from digital devices or other electronic storage  
10 media, all under Rule 41(e)(2)(B).

11 **i. Probable Cause**

12 70. Based upon my review of the evidence gathered in this investigation, my review  
13 of data and records, information received from other agents and computer forensics examiners,  
14 and my training and experience, I submit that if a digital device or other electronic storage  
15 media is found at the search locations described in Attachment A, there is probable cause to  
16 believe that evidence, fruits, and/or instrumentalities of the crimes: 18 U.S.C. § 371  
17 (Conspiracy to Commit Tax Evasion and to defraud the United States); 26 U.S.C. § 7201 (Tax  
18 Evasion); 26 U.S.C. § 7206(1) (Making or Subscribing False Income Tax Returns), will be  
19 stored on those digital devices or other electronic storage media. The evidence collected to  
20 date establishes probable cause to believe that digital devices or other electronic storage are  
21

22 <sup>19</sup> "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not  
23 limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral  
24 input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media,  
25 related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless  
communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants  
("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or  
portable media players.

26 <sup>20</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded.  
27 Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.  
28



1 being used or have been used during the course of the underlying scheme, to, among other  
2 things:

3 a. Create and store documents (i.e., spreadsheets, electronic invoices,  
4 electronic representations of checks or other payment items, and the like) representing  
5 purchases and sales of Salal for Eagle Mountain Products;

6 b. create and store documents representing income and expenses for Eagle  
7 Mountain Products;

8 c. create and store documents reflecting the location of personal assets and  
9 cash;

10 d. create and store documents reflecting international travel;

11 e. create and store documents reflecting purchases of personal items with  
12 nominee accounts;

13 f. create and store documents related to the preparation of tax returns;

14 g. create and store communications with accountant and bookkeeper.

15 71. There is, therefore, probable cause to believe that evidence, fruits and  
16 instrumentalities of the crimes of 18 U.S.C. § 371 (Conspiracy to Commit Tax Evasion and to  
17 defraud the United States); 26 U.S.C. § 7201 (Tax Evasion); 26 U.S.C. § 7206(1) (Making or  
18 Subscribing False Income Tax Returns) will be found on digital devices or other electronic  
19 storage media at the search locations in attachment A, for the following reasons:

20 a. Based on my knowledge, training, and experience, I know that computer  
21 files or remnants of such files can be recovered months or even years after they have been  
22 downloaded onto a digital device or other electronic storage medium, deleted, or viewed via  
23 the Internet. Electronic files downloaded to a digital device or other electronic storage medium  
24 can be stored for years at little or no cost. Even when files have been deleted, they can be  
25 recovered months or years later using forensic tools. This is so because when a person  
26 "deletes" a file on a digital device or other electronic storage media, the data contained in the  
27 file does not actually disappear; rather, that data remains on the storage medium until it is  
28 overwritten by new data.

27 b. Therefore, deleted files, or remnants of deleted files, may reside in free  
28 space or slack space-that is, in space on the digital device or other electronic storage medium  
that is not currently being used by an active file-for long periods of time before they are

1 overwritten. In addition, a computer's operating system may also keep a record of deleted data  
2 in a "swap" or "recovery" file.

3 c. Wholly apart from user-generated files, computer storage media, in  
4 particular, computers' internal hard drives, contain electronic evidence of how a computer has  
5 been used, what it has been used for, and who has used it. To give a few examples, this  
6 forensic evidence can take the form of operating system configurations, artifacts from  
7 operating systems or application operations, file system data structures, and virtual memory  
8 "swap" or paging files. Computer users typically do not erase or delete this evidence, because  
9 special software is typically required for that task. However, it is technically possible to delete  
10 this information.

11 d. Similarly, files that have been viewed via the Internet are sometimes  
12 automatically downloaded into a temporary Internet directory or "cache."

13 72. Based on actual inspection of the federal income tax returns filed with the IRS  
14 during the course of this investigation, I am aware that digital devices and other electronic  
15 storage media were used to generate, store, and transmit documents used in offenses executed  
16 by Leonar Salazar and Eulalia Salazar, that is, Title 18, United States Code, § 371(k),  
17 Conspiracy to Commit Tax Evasion; Title 26, United States Code, § 7201 Attempt to Evade or  
18 Defeat Income Tax; Title 26, United States Code, § 7206(1) Making or Subscribing False  
19 Income Tax Returns. Based on the scope of the investigation, I believe it is likely that Leonar  
20 Salazar and Eulalia Salazar will continue to have some records related to the underlying  
21 scheme and the proceeds generated by the scheme in both paper and electronic formats. This  
22 is because a scheme of this scope requires substantial records to keep track of the various  
23 aspects, including purchases, sales, profits, expenses, etc. Criminals, even when fully aware of  
24 ongoing investigations, frequently keep these records for long periods of time. Especially  
25 sensitive records may be maintained in electronic storage devices such as hidden thumb drives  
26 or other portable media (including smart phones and other more easily concealed devices).  
27 Likewise, with regard to any personal computers found in the business, residence or  
28 automobiles, evidence of Leonar Salazar's and Eulalia Salazar's entire financial life –  
including money spent on everyday goods, travel, leisure, cultural activities, restaurants,  
investments, gifts, house repairs, electronics, automobiles, and real estate, to give just some



1 examples -- would be relevant to the investigation for tax evasion. Therefore, I believe there is  
2 reason to believe that digital devices or electronic storage media currently located at the  
3 Search Locations may contain some or all of the items to be seized in Attachment B.

4 **ii. Forensic Evidence**

5 73. As further described in Attachment B, this application seeks permission to locate  
6 not only computer files that might serve as direct evidence of the crimes described on the  
7 warrant, but also for forensic electronic evidence that establishes how digital devices or other  
8 electronic storage media were used, the purpose of their use, who used them, and when. There  
9 is probable cause to believe that this forensic electronic evidence will be on any digital devices  
10 or other electronic storage media located at the search locations for the following reasons:

11 a. Stored data can provide evidence of a file that was once on the digital  
12 device or other electronic storage media but has since been deleted or edited, or of a deleted  
13 portion of a file (such as a paragraph that has been deleted from a word processing file).  
14 Virtual memory paging systems can leave traces of information on the digital device or other  
15 electronic storage media that show what tasks and processes were recently active. Web  
16 browsers, e-mail programs, and chat programs store configuration information that can reveal  
17 information such as online nicknames and passwords. Operating systems can record  
18 additional information, such as the history of connections to other computers, the attachment  
19 of peripherals, the attachment of USB flash storage devices or other external storage media,  
20 and the times the digital device or other electronic storage media was in use. Computer file  
21 systems can record information about the dates files were created and the sequence in which  
22 they were created.

23 b. As explained herein, information stored within a computer and other  
24 electronic storage media may provide crucial evidence of the "who, what, why, when, where,  
25 and how" of the criminal conduct under investigation, thus enabling the United States to  
26 establish and prove each element or alternatively, to exclude the innocent from further  
27 suspicion. In my training and experience, information stored within a computer or storage  
28 media (e.g., registry information, communications, images and movies, transactional  
information, records of session times and durations, internet history, and anti-virus, spyware,  
and malware detection programs) can indicate who has used or controlled the computer or  
storage media. This "user attribution" evidence is analogous to the search for "indicia of  
occupancy" while executing a search warrant at a residence. The existence or absence of anti-  
virus, spyware, and malware detection programs may indicate whether the computer was  
remotely accessed, thus inculcating or exculpating the computer owner and/or others with  
direct physical access to the computer. Further, computer and storage media activity can



1 indicate how and when the computer or storage media was accessed or used. For example, as  
 2 described herein, computers typically contain information that log: computer user account  
 3 session times and durations, computer activity associated with user accounts, electronic  
 4 storage media that connected with the computer, and the IP addresses through which the  
 5 computer accessed networks and the internet. Such information allows investigators to  
 6 understand the chronological context of computer or electronic storage media access, use, and  
 7 events relating to the crime under investigation.<sup>21</sup> Additionally, some information stored  
 8 within a computer or electronic storage media may provide crucial evidence relating to the  
 9 physical location of other evidence and the suspect. For example, images stored on a  
 10 computer may both show a particular location and have geolocation information incorporated  
 11 into its file data. Such file data typically also contains information indicating when the file or  
 12 image was created. The existence of such image files, along with external device connection  
 13 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
 14 camera or cellular phone with an incorporated camera). The geographic and timeline  
 15 information described herein may either inculcate or exculpate the computer user. Last,  
 16 information stored within a computer may provide relevant insight into the computer user's  
 17 state of mind as it relates to the offense under investigation. For example, information within  
 18 the computer may indicate the owner's motive and intent to commit a crime (e.g., internet  
 19 searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping"  
 20 program to destroy evidence on the computer or password protecting/encrypting such evidence  
 21 in an effort to conceal it from law enforcement).

22 c. A person with appropriate familiarity with how a digital device or other  
 23 electronic storage media works can, after examining this forensic evidence in its proper  
 24 context, draw conclusions about how the digital device or other electronic storage media were  
 25 used, the purpose of their use, who used them, and when.

26 d. The process of identifying the exact files, blocks, registry entries, logs, or  
 27 other forms of forensic evidence on a digital device or other electronic storage media that are  
 28 necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify  
 in advance the records to be sought, digital evidence is not always data that can be merely  
 reviewed by a review team and passed along to investigators. Whether data stored on a  
 computer is evidence may depend on other information stored on the computer and the  
 application of knowledge about how a computer behaves. Therefore, contextual information  
 necessary to understand other evidence also falls within the scope of the warrant.

---

<sup>21</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

1 e. Further, in finding evidence of how a digital device or other electronic  
2 storage media was used, the purpose of its use, who used it, and when, sometimes it is  
3 necessary to establish that a particular thing is not present. For example, the presence or  
4 absence of counter-forensic programs or anti-virus programs (and associated data) may be  
relevant to establishing the user's intent.

5 **A. DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

6 74. I know that when an individual uses either a business or personal computer in  
7 keeping records or filing false tax returns, the individual's personal computers often will serve  
8 both as instrumentalities for committing the crime and storage media for evidence of the  
9 crime. Based on the information in this Affidavit, I believe that the digital devices at the search  
10 locations described in Attachment A are instrumentalities of crime as well as storage devices,  
11 because they constitute the means by which Leonar Salazar and Eulalia Salazar committed the  
12 violations. Any personal computers at the search locations likely were used to commit the  
13 crime of tax evasion because they were used by Salazar and Eulalia (a) to keep financial  
14 records of profits and receipts from business, which he did not disclose by depositing such  
15 funds with third party record keepers, such as banks or brokerage houses; (b) to prepare tax  
16 documents; (c) to keep other records of Salazar's and Eulalia's financial life that individuals  
17 generally rely on banks, brokerage houses, and financial institutions to maintain; and (d) or  
18 otherwise make payments electronically from business or nominee accounts. Therefore, I  
19 believe that in addition to seizing the digital devices to conduct a search of their contents as set  
20 forth herein, there is probable cause to seize those digital devices as instrumentalities of the  
21 criminal activity.

22 75. If, after conducting its examination, law enforcement personnel determine that  
23 any digital device is any instrumentality of the criminal offenses referenced above, the  
24 government may retain that device during the pendency of the case as necessary to, among  
25 other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and  
26 litigate the issue of forfeiture. If law enforcement personnel determine that a device was not  
27 an instrumentality of the criminal offenses referenced above, it shall be returned to the  
28



1 person/entity from whom it was seized within 90 days of the issuance of the warrant, unless  
2 the government seeks and obtains authorization from the Court for its retention.

3 **B. PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

4 76. Because of the nature of the evidence that I am attempting to obtain and the  
5 nature of the investigation, I have not made any prior efforts to obtain the evidence based on  
6 the consent of any party who may have authority to consent. Specifically, I believe that if  
7 Salazar, Eulalia, federal tax return preparer Carlota Herrera, or others who may be involved in  
8 the above-described criminal activity become aware of the investigation in advance of the  
9 execution of a search warrant, they may attempt to destroy any potential evidence, whether  
10 digital or non-digital, thereby hindering law enforcement agents from the furtherance of the  
11 criminal investigation.

12 **C. RISK OF DESTRUCTION OF EVIDENCE**

13 77. I know, based on my training and experience, that digital information can be  
14 very fragile and easily destroyed. Digital information can also be easily encrypted or  
15 obfuscated such that review of the evidence would be extremely difficult, and in some cases  
16 impossible. I do not know whether in the instant case, Leonar Salazar, Eulalia Salazar or  
17 others to whom they may have entrusted their records, used encryption on the computer  
18 systems they utilizes to engage in their crimes. If an encrypted computer is either powered off,  
19 or if the user has not entered the encryption password and logged onto the computer, it is  
20 likely that any information contained on the computer will be impossible to decipher. If the  
21 computer is powered on, however, and the user is already logged onto the computer, there is a  
22 much greater chance that the digital information can be extracted from the computer. This is  
23 because when the computer is on and in use, the password has already been entered and the  
24 data on the computer is accessible. However, giving the owner of the computer time to  
25 activate a digital security measure, pull the power cord from the computer, or even log off of  
26 the computer, could result in a loss of digital information that could otherwise have been  
27 extracted from the computer.  
28



**D. REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS**

78. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

1 **E. SEARCH TECHNIQUES**

2 79. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
3 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or  
4 otherwise copying digital devices or other electronic storage media that reasonably appear  
5 capable of containing some or all of the data or items that fall within the scope of Attachment  
6 B to this Affidavit, and will specifically authorize a later review of the media or information  
7 consistent with the warrant.

8 80. At this time, I believe that Leonar Salazar lives at 3012 93<sup>rd</sup> Avenue SW,  
9 Olympia, WA 98512. Based on my investigation no other people live at this residence.  
10 Because Salazar has at least one minor child, it is possible that the 3012 93<sup>rd</sup> Avenue SW,  
11 Olympia, WA 98512 location will contain digital devices or other electronic storage media  
12 that are predominantly used, and perhaps owned, by persons who are not suspected of a crime.  
13 At this time, I believe that Eulalia Salazar lives at 150 S. Elderberry Ave. Forks, WA 98331.  
14 Based on my investigation, Eulalia's husband and at least three minor children live at the 150  
15 S. Elderberry Ave. Forks, WA 98331, which gives the possibility that the location will contain  
16 digital devices or other electronic storage media that are predominately used and perhaps  
17 owned, by persons who are not suspected of a crime. If agents conducting the search  
18 nonetheless determine that it is possible that the things described in this warrant could be  
19 found on those computers or digital devices, this application seeks permission to search and if  
20 necessary to seize those computers and digital devices as well. It may be impossible to  
21 determine, on scene, which computers contain the things described in this warrant.

22 81. EMP is a functioning company that may well conduct legitimate business. The  
23 seizure of the Company's computers may limit the Company's ability to conduct its legitimate  
24 business. As with any search warrant, I expect that this warrant will be executed reasonably.  
25 Reasonable execution will likely involve conducting an investigation on the scene of what  
26 computers, or storage media, must be seized or copied, and what computers or storage media  
27 need not be seized or copied. Where appropriate, officers will copy data, rather than  
28 physically seize computers, to reduce the extent of disruption. If employees of the Company



1 so request, the agents will, to the extent practicable, attempt to provide the employees with  
2 copies of data that may be necessary or important to the continuing function of the Company's  
3 legitimate business. If, after inspecting the computers, it is determined that some or all of this  
4 equipment is no longer necessary to retrieve and preserve the evidence, the government will  
5 return it.

6 82. Consistent with the above, I am requesting the authority to seize and/or obtain a  
7 forensic image of digital devices or other electronic storage media that reasonably appear  
8 capable of containing data or items that fall within the scope of Attachment B to this Affidavit,  
9 and to conduct off-site searches of the digital devices or other electronic storage media and/or  
10 forensic images, using the following procedures:

11 **a. Securing the Data:**

12 i. Upon securing the physical search site, the search team will  
13 conduct an initial review of any digital devices or other electronic storage media located at the  
14 subject premises described in Attachment A that are capable of containing data or items that  
15 fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure  
16 the data contained on these devices onsite in a reasonable amount of time and without  
17 jeopardizing the ability to accurately preserve the data.

18  
19 ii. In order to examine the electronically stored information ("ESI")  
20 in a forensically sound manner, law enforcement personnel with appropriate expertise will  
21 attempt to produce a complete forensic image, if possible and appropriate, of any digital  
22 device or other electronic storage media that is capable of containing data or items that fall  
23 within the scope of Attachment B to this Affidavit.<sup>22</sup>

24  
25  
26 <sup>22</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other  
27 electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific  
28 procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate  
these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their  
search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise



1                   iii.     A forensic image may be created of either a physical drive or a  
2 logical drive. A physical drive is the actual physical hard drive that may be found in a typical  
3 computer. When law enforcement creates a forensic image of a physical drive, the image will  
4 contain every bit and byte on the physical drive. A logical drive, also known as a partition, is  
5 a dedicated area on a physical drive that may have a drive letter assigned (for example the c:  
6 and d: drives on a computer that actually contains only one physical hard drive). Therefore,  
7 creating an image of a logical drive does not include every bit and byte on the physical drive.  
8 Law enforcement will only create an image of physical or logical drives physically present on  
9 or within the subject device. Creating an image of the devices located at the search locations  
10 described in Attachment A will not result in access to any data physically located elsewhere.  
11 However, digital devices or other electronic storage media at the search locations described in  
12 Attachment A that have previously connected to devices at other locations may contain data  
13 from those other locations.

14  
15                   iv.     In addition to creating an image of a physical or logical drive from  
16 a digital device or other electronic storage media, law enforcement may attempt to create an  
17 image of the random access memory (RAM) of a digital device. Agents may only create an  
18 image of a digital device's RAM if the computer is powered on at the time of the search. This  
19 is because RAM is only active when the device is in operation. Any data contained in the  
20 RAM will be lost when the computer is powered off. A computer's RAM may contain  
21 evidence related to who else is logged onto the computer (even remotely), open connections  
22 that might indicate a program is waiting for commands, passwords for encryption programs,  
23 hardware and software settings, maps of recent files and applications accessed, and  
24 information related to what communication vendors have recently been utilized on the device

25  
26 that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative  
27 expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic  
28 examiners and investigative personnel work closely together.

1 (i.e. instant messaging services, e-mail services, social networking sites, etc.). In addition,  
2 RAM may contain encryption keys necessary to access other elements of the subject device.

3  
4 v. If based on their training and experience, and the resources  
5 available to them at the search site, the search team determines it is not practical to make an  
6 on-site image within a reasonable amount of time and without jeopardizing the ability to  
7 accurately preserve the data, then the digital devices or other electronic storage media will be  
8 seized and transported to an appropriate law enforcement laboratory to be forensically imaged  
9 and reviewed.

10 **b. Searching the Forensic Images:**

11 i. Searching the forensic images for the items described in  
12 Attachment B may require a range of data analysis techniques. In some cases, it is possible for  
13 agents and analysts to conduct carefully targeted searches that can locate evidence without  
14 requiring a time-consuming manual search through unrelated materials that may be  
15 commingled with criminal evidence. In other cases, however, such techniques may not yield  
16 the evidence described in the warrant, and law enforcement may need to conduct more  
17 extensive searches to locate evidence that falls within the scope of the warrant. The search  
18 techniques that will be used will be only those methodologies, techniques and protocols as  
19 may reasonably be expected to find, identify, segregate and/or duplicate the items authorized  
20 to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may  
21 necessarily expose many or all parts of a hard drive to human inspection in order to determine  
22 whether it contains evidence described by the warrant.

23  
24 ii. These methodologies, techniques and protocols may include the  
25 use of a "hash value" library to exclude normal operating system files that do not need to be  
26 further searched.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## VI. CONCLUSION

83. Based on my experience and the facts set forth in this Affidavit, I believe there is probable cause to believe documents and records, which are evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy to Commit Tax Evasion and to defraud the United States); 26 U.S.C. § 7201 (Tax Evasion); 26 U.S.C. § 7206(1) (Making or Subscribing False Income Tax Returns) are maintained at the following locations which are described with particularity in Attachment A:

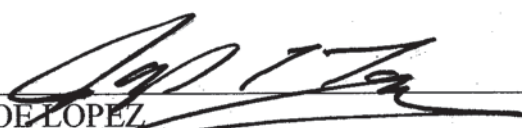
a. a. The offices of Eagle Mountain Products, Inc., located at or near 213 W. Wallace Kneeland Blvd. Shelton, WA 98584; and

b. Leonar Salazar's residence, located at 3012 93<sup>rd</sup> Ave. SW Olympia, WA 98512; and

c. Eulalia Salazar's residence, located at 150 S. Elderberry Ave. Forks, WA 98331; and

d. Acura MDX with Washington license plate number AXY4781 and Vehicle Identification Number 2HNYD2H26AH528903; and

e. Nissan Titan Pickup with Washington license plate number B37590T and Vehicle Identification Number 1N6AA07BX5N554954

  
JOE LOPEZ  
Special Agent, Criminal Investigation  
Internal Revenue Service

SUBSCRIBED AND SWORN to before me this 3<sup>rd</sup> day of June, 2016.

  
DAVID W. CHRISTEL  
United States Magistrate Judge